④

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-249967
(43)Date of publication of application : 17.09.1999

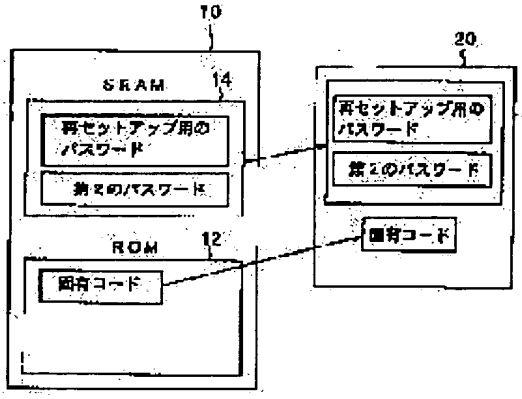
(51)Int.CI. G06F 12/14
G06F 12/16

(21)Application number : 10-061888
(22)Date of filing : 27.02.1998

(71)Applicant : FANUC LTD
(72)Inventor : FUJIBAYASHI KENTARO
HISHIKAWA TETSUO
TANOSAKI EIJI

(54) METHOD FOR PREVENTING UNJUST COPY OF NC DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent peculiar data set up by an NC maker from being copied and unjustly used and to enable a legal user to smoothly perform the restoration work of a numerical controller.
SOLUTION: When backup data of an SRM 14 is preserved in a memory card 20, a peculiar code of a ROM 12 is written in the memory card 20. When backup information is set up again, it is discriminated whether a peculiar code of a numerical controller 10 is matched with the peculiar code of the memory card 20 or not, and backup information is permitted to be set up again only in the case of coincidence between them, thereby preventing backup data generated in another numerical controller from being unjustly taken in.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－249967

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｆ
	12/16	３１０		12/16	３１０Ｍ

審査請求　未請求　請求項の数３　ＦＤ　（全 11 頁）

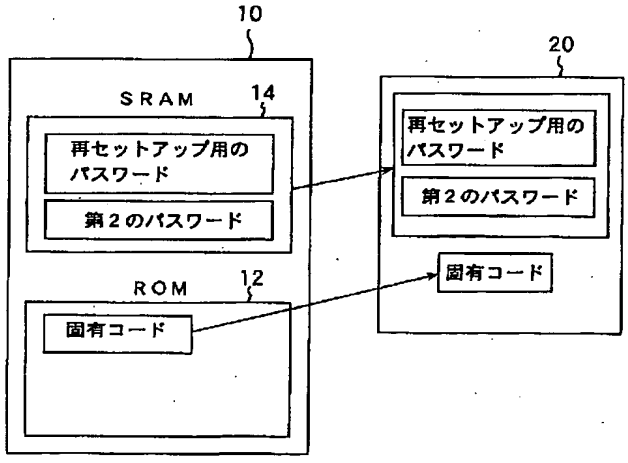
(21)出願番号　特願平10－61888

(22)出願日　平成10年(1998)２月27日

(71)出願人　390008235
ファナック株式会社
山梨県南都留郡忍野村忍草字古馬場3580番地
(72)発明者　藤林　謙太郎
山梨県南都留郡忍野村忍草字古馬場3580番地　ファナック株式会社内
(72)発明者　菱川　哲夫
山梨県南都留郡忍野村忍草字古馬場3580番地　ファナック株式会社内
(72)発明者　田野崎　英司
山梨県南都留郡忍野村忍草字古馬場3580番地　ファナック株式会社内
(74)代理人　弁理士　竹本　松司　（外４名）

(54)【発明の名称】　ＮＣデータの不正複写防止方法

(57)【要約】
【課題】　ＮＣメーカーでセットアップした固有のデータが複写されて不正利用されるのを防止し、かつ、正当なユーザーによる数値制御装置の復旧作業を円滑化する。
【解決手段】　ＳＲＡＭ１４のバックアップデータをメモリカード２０に保存する際に、ＲＯＭ１２の固有コードがメモリカード２０にに書き込まれるようにしておく。バックアップ情報の再セットアップに際しては、その数値制御装置１０の固有コードがメモリカード２０の固有コードと一致しているか否かを判別し、一致する場合にだけ再セットアップ作業を許容することで、別の数値制御装置で生成されたバックアップデータの不正な持ち込みを禁止する。



1

【特許請求の範囲】

【請求項１】　数値制御装置に必要とされる不揮発性ＲＡＭの情報のバックアップを外部記憶媒体に保存する機能と、前記外部記憶媒体のバックアップ情報を不揮発性ＲＡＭに再セットアップする機能とを備えた数値制御装置において、

不揮発性ＲＡＭの情報のバックアップを外部記憶媒体に保存する際に、前記数値制御装置に記憶されている書き換え不能な固有コードが強制的に外部記憶媒体に書き込まれるようにしておき、

バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致している場合にだけ再セットアップ作業を実行するようにしたことを特徴とするＮＣデータの不正複写防止方法。

【請求項２】　再セットアップ用のパスワードが前記固有コードと共に数値制御装置から外部記憶媒体に書き込まれるようにしておき、

バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致していない場合であっても、外部記憶媒体に書き込まれている再セットアップ用のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合には再セットアップ作業を実行するようにしたことを特徴とする請求項１記載のＮＣデータの不正複写防止方法。

【請求項３】　数値制御装置に記憶されている前記再セットアップ用のパスワードを書き換えるための第２のパスワードを数値制御装置に記憶させておき、

数値制御装置に記憶されている第２のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合にだけ前記再セットアップ用のパスワードの書き換えを実行するようにしたことを特徴とする請求項２記載のＮＣデータの不正複写防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＮＣデータの不正複写防止方法に関する。

【０００２】

【従来の技術】数値制御装置の出荷に際しては、その駆動制御に必要とされるオペレーティングシステムや各種パラメータの値またはアプリケーションプログラム等といった重要な情報を予めＮＣメーカーがＳＲＡＭ等の不揮発性ＲＡＭに格納して出荷するのが一般的である。

【０００３】しかし、実際には、数値制御装置の誤動作や誤った操作、例えば、メモリ保護エラーによる書き込み動作や上書き動作等によって、不揮発性ＲＡＭ内のオペレーティングシステムや各種パラメータまたはアプリケーションプログラム等のデータに異常や損傷が生じる場合があり、数値制御装置の復旧作業を円滑に行う必要

2

上、ユーザーサイドで不揮発性ＲＡＭ内の情報をメモリカード等の外部記憶媒体にバックアップして保存することが多い。

【０００４】不揮発性ＲＡＭの情報に損傷を生じた数値制御装置、即ち、ＮＣメーカー側で予めオペレーティングシステムや各種パラメータまたはアプリケーションプログラム等をセットアップして出荷した数値制御装置に対してバックアップ情報の再セットアップ作業を行うことで、その数値制御装置を出荷時と同じ状態に戻して使用することには一向に不都合はないが、そのバックアップ情報を別の数値制御装置に移植して利用するのは、契約条件にもよるが、一般に１ライセンス１商品パッケージの原則からは違法であり、そのような不正な複写行為は何らかの方法で禁止する必要がある。

【０００５】また、このようなバックアップ情報には非公開のソースコード等が含まれる場合が多いので、バックアップ情報を保存したメモリカード等の外部記憶媒体が第三者の手に渡って複写されると、ＮＣメーカーは機密保持の点で大きな損害を被ることになる。

【０００６】

【発明が解決しようとする課題】そこで、本発明の課題は、前記従来技術の欠点を解消し、ＮＣメーカーでセットアップした固有のデータが不用意に複写されて不正に利用されるのを防止し、しかも、正当なユーザーが数値制御装置の復旧作業を円滑に行うことのできるＮＣデータの不正複写防止方法を提供することにある。

【０００７】

【課題を解決するための手段】本発明は、不揮発性ＲＡＭの情報のバックアップを外部記憶媒体に保存する際に、数値制御装置に記憶されている書き換え不能な固有コードが強制的に外部記憶媒体に書き込まれるようにしておき、バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致している場合にだけ再セットアップ作業を実行するようにしたことを特徴とする構成により前記課題を達成した。

【０００８】従って、ある数値制御装置で生成されたバックアップ情報を固有コードが異なる別の数値制御装置に移植することは事実上不可能となり、また、バックアップ情報を生成した数値制御装置に対して正当なユーザーがバックアップ情報を再セットアップする場合には、固有コードの一致によりシリアルナンバー等の入力を省略して円滑な再セットアップ作業を行うことができる。しかも、バックアップ情報を保存した外部記憶媒体には書き換え不能な固有コードが書き込まれるので、外部記憶媒体の不正な持ち出しや貸与があった場合には、その出所、即ち、そのバックアップ情報を生成した数値制御装置を容易に突き止めることができる。

【０００９】また、再セットアップ用のパスワードが前記固有コードと共に数値制御装置から外部記憶媒体に書

き込まれるようにしておき、バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致していない場合であっても、外部記憶媒体に書き込まれている再セットアップ用のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合には再セットアップ作業を実行できるようにすることで、ＮＣメーカーの委託を受けた現地作業員のサービス業務の能率化を図った。

【００１０】例えば、新たなライセンス契約を加入することにより、その時点で既にそのユーザーが他の数値制御装置でライセンスを取得して使用していた機能をその時点でユーザーが保有する別の数値制御装置に付加して利用しようとする場合、ライセンス契約を加えようとする数値制御装置に必要とされるバックアップ情報がその場にない場合でも、ＮＣメーカーの委託を受けて再セットアップ用のパスワードを開示されている現地作業員さえいれば、既存の数値制御装置に他の数値制御装置で生成したバックアップ情報を用いて再セットアップ作業を行うことで数値制御装置に新たな機能を付加することができる。従って、ＮＣメーカーがユーザーから既存の数値制御装置を回収して再セットアップ作業を行う必要はなく、また、ユーザーが保有する既存の数値制御装置の固有コードを調べてその数値制御装置に見合ったバックアップ情報を一々外部記憶媒体に記憶させてユーザーに頒布する必要もなくなり、ライセンスの更新作業を円滑に行うことができる。しかも、ライセンスを更新した数値制御装置で生成されたバックアップ情報を外部記憶媒体に保存する際には、その数値制御装置自体の固有コードが書き込まれることになるので、一旦ライセンスを更新してしまえば、その数値制御装置に異常が発生した場合の再セットアップ作業はユーザー自身の手で簡単に行うことができる。

【００１１】更に、数値制御装置に記憶されている再セットアップ用のパスワードを書き換えるための第２のパスワードを数値制御装置に記憶させておき、数値制御装置に記憶されている第２のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合にだけ再セットアップ用のパスワードの書き換えを実行できるようにしたことで、現地作業員の信頼性の低下に伴うＮＣメーカー側の危険負担を小さくした。

【００１２】ＮＣメーカーのみが知る第２のパスワードを使用して再セットアップ用のパスワードを書き換えれば、その数値制御装置で生成されたバックアップ情報に含まれる再セットアップ用のパスワードと現地作業員が以前に知らされた再セットアップ用のパスワードとが異なるようになるので、その数値制御装置で生成されたバックアップ情報を他の数値制御装置に移植することは現地作業員にもできなくなる。また、第２のパスワードによって再セットアップ用のパスワードの書き換えがプロテクトされるため、何らかの方法で不正な複写作業が行

われた場合でも再セットアップ用のパスワード自体は外部記憶媒体またはそのデータを複写された数値制御装置にそのまま残ることになり、再セットアップ用のパスワードを確認することにより、そのバックアップ情報を生成した数値制御装置や不正な作業を行った現地作業員を容易に突き止めることができる。

【００１３】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図１は本発明の不正複写防止方法を適用した一実施形態の数値制御装置１０と該数値制御装置１０によって駆動制御される工作機械の要部を示すブロック図である。

【００１４】プロセッサ１１は数値制御装置１０を全体的に制御するプロセッサであり、ＲＯＭ１２に格納されたシステムプログラムをバス２１を介して読み出し、このシステムプログラムに従って、数値制御装置１０を全体的に制御する。ＲＡＭ１３には一時的な計算データ、表示データ等が格納される。

【００１５】ＳＲＡＭ１４は図示しないバッテリでバックアップされ、数値制御装置１０の電源がオフにされても記憶状態が保持される不揮発性ＲＡＭとして構成され、ＮＣメーカーでセットアップしたデータ、例えば、オペレーティングシステムや各種パラメータまたはアプリケーションプログラム等に関連した重要な情報が格納されている。

【００１６】インターフェイス１５は外部機器用のインターフェイスであり、外部記憶媒体となるメモリカード２０に対してデータの読み書きを行うためのドライブユニット７２が接続され、ＳＲＡＭ１４からメモリカード２０へのデータのバックアップ作業や、メモリカード２０からＳＲＡＭ１４へのデータの再セットアップ作業が実施できるようになっている。

【００１７】ＳＲＡＭ１４からメモリカード２０へのデータのバックアップ作業に必要とされるエンコードや圧縮およびデータ書き出し用のプログラムと、メモリカード２０からＳＲＡＭ１４へのデータの再セットアップ作業に必要とされる解凍やデコードおよびデータ書き込み用のプログラムは、各々ＲＯＭ１２に格納されている。

【００１８】また、装置のシリアルナンバー等で構成される数値制御装置１０の固有コードは書き換え不能な状態でＲＯＭ１２に格納され、再セットアップ用のパスワード、および、このパスワードを書き換えるための第２のパスワードの各々は、数値制御装置１０の出荷段階で予めＮＣメーカーによってＳＲＡＭ１４に登録されている。

【００１９】このうち装置の出荷段階で最初にＳＲＡＭ１４に登録した再セットアップ用のパスワード、または、その後でＮＣメーカーが書き換えた再セットアップ用のパスワードの内容に関してはＮＣメーカーがサービス業務を委託する現地作業員に対して開示するが、再セ

ットアップ用のパスワードを書き換えるための第２のパスワードの情報に関してはＮＣメーカー内部で秘匿するようにする。

【００２０】ＰＭＣ（プログラマブル・マシン・コントローラ）１６は数値制御装置１０に内蔵されたシーケンスプログラムで工作機械を制御する。即ち、加工プログラムで指令された機能に従って、これらシーケンスプログラムで工作機械側で必要な信号に変換し、Ｉ／Ｏユニット１７から工作機械側に出力する。この出力信号により工作機械側の各種アクチュエータが作動する。また、工作機械側のリミットスイッチおよび機械操作盤の各種スイッチ等の信号を受けて、必要な処理をしてプロセッサ１１に渡す。

【００２１】各軸の現在位置、アラーム、画像データ等の信号はＣＲＴ／ＭＤＩユニット７０の表示装置に送られ、表示装置に表示される。インターフェイス１８はＣＲＴ／ＭＤＩユニット７０のキーボードからのデータを受けてプロセッサ１１に渡す。インターフェイス１９は手動パルス発生器７１に接続され、手動パルス発生器７１からのパルスを受ける。手動パルス発生器７１は工作機械側の機械操作盤に実装され、手動で機械可動部を精密に位置決めするために使用される。

【００２２】軸制御回路３０～３２はプロセッサ１１からの各軸の移動指令を受けて、各軸の指令をサーボアンプ４０～４２に出力する。サーボアンプ４０～４２はこの指令を受けて各軸のサーボモータ５０～５２を駆動する。Ｘ，Ｙ，Ｚ各軸のサーボモータ５０～５２には位置速度検出用のパルスコーダが内蔵されており、このパルスコーダからのフィードバック信号が軸制御回路３０～３２にフィードバックされる。軸制御回路３０～３２に内蔵されたサーボ制御ＣＰＵの各々はこれらのフィードバック信号と前述の移動指令とに基いて位置ループ、速度ループ、電流ループの各処理を行い、最終的な駆動制御のためのトルク指令を各軸毎に求めて各軸のサーボモータ５０～５２の位置、速度を制御する。

【００２３】スピンドル制御回路６０はスピンドル回転指令およびスピンドルのオリエンテーション等の指令を受けて、スピンドルアンプ６１にスピンドル速度信号を出力する。スピンドルアンプ６１はこのスピンドル速度信号を受けて、スピンドルモータ６２を指令された回転速度で回転させる。また、オリエンテーション指令によって所定の位置にスピンドルモータ６２の回転位置を位置決めする。

【００２４】図２はバックアップ作業時における数値制御装置１０の処理の概略を示す概念図である。

【００２５】前述した通り、データのバックアップ作業に必要とされるエンコードや圧縮およびデータ書き出し用のプログラムはＲＯＭ１２に格納されており、ドライブユニット７２にメモリカード２０をセットしてＣＲＴ／ＭＤＩユニット７０からバックアップデータ作成指令

を入力することにより、プロセッサ１１が、ＳＲＡＭ１４からメモリカード２０へのデータの書き出し作業と、それに伴うエンコードや圧縮作業を開始する。

【００２６】このとき、数値制御装置１０の固有コードがＲＯＭ１２から読み出されてメモリカード２０に保存され、ＳＲＡＭ１４に登録されている再セットアップ用のパスワードと第２のパスワードは、ＳＲＡＭ１４内のオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等と共にメモリカード２０に書き出される。

【００２７】従って、数値制御装置１０の誤動作やアラートを無視したオペレターの誤操作等によってＳＲＡＭ１４内のオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に損傷が生じた場合には、メモリカード２０にバックアップデータとして保存されている情報をそのままＳＲＡＭ１４に再セットアップすることで数値制御装置１０の障害復旧を行うことができる。

【００２８】図３は再セットアップ作業時におけるプロセッサ１１の処理動作を示すフローチャートである。

【００２９】作業者がＣＲＴ／ＭＤＩユニット７０から再セットアップ指令を入力すると、これを検出したプロセッサ１１は、ＳＲＡＭ１４をクリアし、ドライブユニット７２にメモリカード２０をセットする旨のガイダンスメッセージをＣＲＴ／ＭＤＩユニット７０に表示して（ステップａ１）、メモリカード２０の挿入を待つ待機状態に入る（ステップａ２）。

【００３０】そして、メモリカード２０が挿入されると、これを検出したプロセッサ１１は、メモリカード２０に保存されているデータのうち数値制御装置の固有コードに関連した部分のデータをメモリカード２０からＲＡＭ１３に読み込んで解凍およびデコードに関する処理を実行し、メモリカード２０に保存されていた数値制御装置の固有コードとＲＯＭ１２に登録されている固有コードとを比較して（ステップａ３）、両者が一致しているか否かを判別する（ステップａ４）。

【００３１】一致している場合には、メモリカード２０に保存されているバックアップデータがこの数値制御装置１０によって生成されたバックアップデータであって、ユーザーによる合法的な再セットアップ作業が行われようとしていることを意味するので、プロセッサ１１は、引き続きメモリカード２０からオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連したデータを読み込んで解凍およびデコードに関する処理を実行し、復元されたデータとメモリカード２０に登録されている２つのパスワードを数値制御装置１０のＳＲＡＭ１４に書き込んで、ＳＲＡＭ１４内のデータを損傷発生前の状態に復旧させる（ステップａ９）。

【００３２】また、メモリカード２０に保存されていた

数値制御装置の固有コードとＲＯＭ１２に登録されている固有コードとが一致せずにステップａ４の判別結果が偽となった場合、プロセッサ１１は、更に、再セットアップ用のパスワードを入力する旨のガイダンスメッセージをＣＲＴ／ＭＤＩユニット７０に表示して（ステップａ５）、パスワードの入力を待つ待機状態に入る（ステップａ６）。

【００３３】そして、作業者がＣＲＴ／ＭＤＩユニット７０のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ１１は、メモリカード２０に保存されているデータのうち再セットアップ用のパスワードに関連した部分のデータをメモリカード２０からＲＡＭ１３に読み込んで解凍およびデコードに関する処理を実行し、作業者が入力したパスワードとメモリカード２０に保存されていた再セットアップ用のパスワードとを比較し（ステップａ７）、両者が一致しているか否かを判別する（ステップａ８）。

【００３４】一致している場合には、再セットアップ作業を行おうとしている作業者が再セットアップ用のパスワードを知っていること、即ち、ＮＣメーカーのサービス業務を委託された現地作業員であることを意味するので、プロセッサ１１は、引き続きメモリカード２０からオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連したデータを読み込んで解凍およびデコードに関する処理を実行し、復元されたデータとメモリカード２０に登録されている２つのパスワードを数値制御装置１０のＳＲＡＭ１４に書き込む（ステップａ９）。

【００３５】この場合は、メモリカード２０に保存されていた数値制御装置の固有コードとＲＯＭ１２に登録されている固有コードとが相違しても再セットアップ作業の実施が可能である。従って、メモリカード２０に保存されているデータは、最初にＮＣメーカーがその数値制御装置１０にセットアップしたものと同じであるとは限らず、オペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連した新たな機能がＳＲＡＭ１４に追加される場合がある。

【００３６】例えば、既存の数値制御装置１０に対し、より新しい他の数値制御装置で生成したバックアップ情報を用いて再セットアップ作業を行うことによって新たな機能を付加するといった場合がある。この作業を実施できるのは、再セットアップ用のパスワードを開示された現地作業員のみであり、このようなサービスを受けるためには、当然、ユーザーとメーカーとの間で新たなライセンス契約の更新が必要となる。

【００３７】このようにして異なる固有コードを有するメモリカード２０から再セットアップ作業を行って新規機能を追加した場合であっても、数値制御装置１０のＳＲＡＭ１４からメモリカード２０にバックアップを保存する際には、その数値制御装置１０自体の固有コードがＲＯＭ１２からメモリカード２０に保存されることになるので、もし、後々その数値制御装置１０のＳＲＡＭ１４に損傷が生じたような場合には、再セットアップ用のパスワードを知らないユーザーでも、その数値制御装置１０からバックアップデータを保存されたメモリカード２０を用いて再セットアップ作業を行うことで、固有コードの一致によりＳＲＡＭ１４の損傷を簡単に復旧することができる。

【００３８】また、再セットアップ用のパスワードを使用して再セットアップ作業を実施した場合、その時に使用されたパスワードの値が再セットアップの対象となった数値制御装置１０のＳＲＡＭ１４にそのまま保存されるので、現地作業員が違法な手続きで再セットアップ作業を行ったような場合、例えば、ライセンス契約を更新せずに他の数値制御装置のＳＲＡＭ１４の内容を数値制御装置１０に無断複写したような場合、メーカー側は、ＳＲＡＭ１４に保存されている再セットアップ用のパスワードを調べることにより、そのパスワードを使用している現地作業員、即ち、違法な複写作業を行った現地作業員を容易に特定することができる。

【００３９】また、メモリカード２０の側にはそのメモリカード２０にバックアップデータを保存した数値制御装置１０の固有コードが保存されるので、メモリカード２０自体の不正な持ち出しや貸与があった場合にも、その複写元となった数値制御装置１０を容易に特定することができる。

【００４０】メモリカード２０に保存されていた再セットアップ用のパスワードと作業者が入力したパスワードとが一致せずにステップａ８の判別結果が偽となった場合には、再セットアップ作業を行おうとしている作業者が再セットアップ用のパスワードを知らないこと、つまり、ＮＣメーカーのサービス業務を委託された正規の現地作業員以外の人間によって不正な複写作業が行われようとしていることを意味するので、プロセッサ１１は、ステップａ９の再セットアップ処理をキャンセルして処理を終了する。

【００４１】以上の処理により、ユーザーによるデータの不正複写は未然に防止されるが、再セットアップ用のパスワードを知っている現地作業員によるデータの不正複写までは禁止できない。従って、より厳格な管理を望むのであれば、必要に応じてメーカー側で数値制御装置１０を点検し、ＳＲＡＭ１４に不正なデータが持ち込まれていないかどうかを確認する必要がある。

【００４２】つまり、数値制御装置１０のＳＲＡＭ１４に記憶されている再セットアップ用のパスワードが予めメーカーがその数値制御装置１０にセットアップしたパスワードと一致していれば、その数値制御装置１０においてＳＲＡＭ１４の内容に損傷を生じた経歴が皆無であるか、または、損傷が生じた経歴があったとしてもその損傷を修復するためにその数値制御装置１０自体で生成

したバックアップデータをユーザーが再セットアップしたかのどちらかであり、いずれの場合も問題となる点はない。

【００４３】一方、数値制御装置１０のＳＲＡＭ１４に記憶されている再セットアップ用のパスワードと予めメーカーがその数値制御装置１０にセットアップしたパスワードとが一致していなければ、少なくとも、現地作業員が再セットアップ用のパスワードを使用して別の数値制御装置からバックアップデータを持ち込んだことは明らかとなる。そして、これによって追加された新機能に関する部分のライセンス契約がユーザーとメーカーとの間で取り交わされていれば合法的な作業であり、また、ライセンス契約が更新されていなければ非合法な作業が行われたことを意味する。

【００４４】図４は数値制御装置１０のＳＲＡＭ１４に記憶されている再セットアップ用のパスワードをメーカー側で確認する場合の処理を示すフローチャートである。

【００４５】作業者がＣＲＴ／ＭＤＩユニット７０からパスワード確認指令を入力すると、これを検出したプロセッサ１１は、パスワード確認用の画面をＣＲＴ／ＭＤＩユニット７０に表示して（ステップｂ１）、第２のパスワードを入力する旨のガイダンスメッセージを表示し（ステップｂ２）、パスワードの入力を待つ待機状態に入る（ステップｂ３）。なお、パスワード確認指令の入力方法に関してはユーザーおよび現地作業員には開示せず、ＮＣメーカー内部で秘匿するようにする。

【００４６】そして、作業者がＣＲＴ／ＭＤＩユニット７０のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ１１は、ＳＲＡＭ１４に登録されている第２のパスワードを読み込み、作業者が入力したパスワードとＳＲＡＭ１４に登録されている第２のパスワードとを比較して（ステップｂ４）、両者が一致しているか否かを判別する（ステップｂ５）。

【００４７】一致している場合には、再セットアップ用のパスワードの確認作業を行おうとしている作業者がＮＣメーカー側の作業者であることを意味するので、プロセッサ１１はＳＲＡＭ１４から再セットアップ用のパスワードを読み込んで、その値をＣＲＴ／ＭＤＩユニット７０に表示して作業者に開示する（ステップｂ６）。

【００４８】また、ＳＲＡＭ１４に登録されている第２のパスワードと作業者が入力したパスワードとが一致せずにステップｂ５の判別結果が偽となった場合には、再セットアップ用のパスワードの確認作業を行おうとしている作業者が第２のパスワードを知らないこと、つまり、ＮＣメーカー側の作業者ではないことを意味するので、プロセッサ１１は、ステップｂ６の表示処理をキャンセルして処理を終了する。

【００４９】前述したように、ステップＢ６の処理で表示された再セットアップ用のパスワードが、メーカーが

その数値制御装置１０に予めセットアップしておいたパスワードと一致していれば問題はないが、相違している場合には、少なくとも、現地作業員が再セットアップ用のパスワードを使用してその数値制御装置１０に別の数値制御装置からバックアップデータを持ち込んだことを意味しているので、メーカー側としては、これによって追加された新機能に関する部分のライセンス契約がユーザーとメーカーとの間で取り交わされているか否かについて調べてみる必要がある。

【００５０】当然、正式なライセンス契約が締結されていれば、新機能の追加に使用したバックアップデータを提供したメモリカード２０の再セットアップ用パスワードの情報はメーカ側で管理されている筈であるから、両者の比較は可能である。

【００５１】ここで正式なライセンス契約が確認されれば問題はないが、確認されない場合には、ＮＣメーカーがサービス業務を委託した現地作業員がメーカー側に無断で違法なデータ複写作業を行ったことを意味する。

【００５２】その現地作業員を突き止めるためにはステップｂ６の処理で表示された再セットアップ用のパスワードの値を確認すればよい。つまり、メーカー側がその再セットアップ用パスワードを開示した現地作業員が違法なデータ複写作業を行った本人である。

【００５３】このような問題が発生して現地作業員の信頼性が低下した場合、再セットアップ用のパスワードの値をそのまま現地作業員が利用できるようにしておくと危険であるから、再セットアップ用のパスワードを更新して従来のパスワードを利用できなくする必要がある。

【００５４】図５および図６は再セットアップ用のパスワードを変更するための処理を示すフローチャートである。

【００５５】まず、作業者がＣＲＴ／ＭＤＩユニット７０からパスワード変更指令を入力すると、これを検出したプロセッサ１１は、パスワード変更用の画面をＣＲＴ／ＭＤＩユニット７０に表示して（ステップｃ１）、第２のパスワードを入力する旨のガイダンスメッセージを表示し（ステップｃ２）、パスワードの入力を待つ待機状態に入る（ステップｃ３）。なお、パスワード変更指令の入力方法に関してはユーザーおよび現地作業員には開示せず、ＮＣメーカー内部で秘匿するようにする。

【００５６】そして、作業者がＣＲＴ／ＭＤＩユニット７０のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ１１は、ＳＲＡＭ１４に登録されている第２のパスワードを読み込み、作業者が入力したパスワードとＳＲＡＭ１４に登録されている第２のパスワードとを比較して（ステップｃ４）、両者が一致しているか否かを判別する（ステップｃ５）。

【００５７】一致していない場合には、再セットアップ用のパスワードの変更作業を行おうとしている作業者が第２のパスワードを知らないこと、即ち、作業者がＮＣ

メーカー側の作業者ではないことを意味しているので、プロセッサ１１は、ステップｃ６以降の処理をキャンセルして処理を終了する。従って、この場合には再セットアップ用のパスワードの変更作業は実行されない。

【００５８】また、ステップｃ５の判別結果が真となってＮＣメーカー側の作業者であることが確認された場合、プロセッサ１１は、更に、それまで使用されていた再セットアップ用のパスワード、つまり、問題が生じて信頼性の低下した再セットアップ用のパスワードを入力する旨のガイダンスメッセージをＣＲＴ／ＭＤＩユニット７０に表示し（ステップｃ６）、それまで使用されていた再セットアップ用のパスワードの入力を待つ待機状態に入る（ステップｃ７）。

【００５９】そして、作業者がＣＲＴ／ＭＤＩユニット７０のキーボード等を介して問題となっているパスワードを入力すると、これを検出したプロセッサ１１は、ＳＲＡＭ１４に記憶されている再セットアップ用のパスワードを読み込み、作業者が入力したパスワードとＳＲＡＭ１４に記憶されている再セットアップ用のパスワードとを比較して（ステップｃ８）、両者が一致しているか否か、つまり、その数値制御装置１０に対しての再セットアップ作業が本当に現時点で問題とされている再セットアップ用のパスワードを用いて実施されたものであるか否かを判別する（ステップｃ９）。

【００６０】問題とされている再セットアップ用のパスワードと数値制御装置１０のＳＲＡＭ１４に記憶されている再セットアップ用のパスワードとが一致しない場合には、その数値制御装置１０に対する再セットアップ作業が問題のない再セットアップ用のパスワードによって実施されていることを意味するので、その再セットアップ用のパスワードを無意味に書き換えるべきではない。

【００６１】従って、ステップｃ９の判別結果が偽となった場合、プロセッサ１１は、ステップｃ１０以降の処理をキャンセルして処理を終了し、再セットアップ用のパスワードの変更作業を実質的に非実行とする。

【００６２】ステップｃ６～ステップｃ９の処理は、ユーザーが多数の数値制御装置を所有するような場合に、正当に使用されている数値制御装置の再セットアップ用パスワードが不用意に別のパスワードに書き換えられるといった事故を防止するためのものである。

【００６３】また、ステップｃ９の判別結果が真となった場合には、その数値制御装置１０に対する再セットアップ作業が現時点で問題とされている再セットアップ用のパスワードによって実施されたことを意味するので、その数値制御装置１０から再び重要な情報が持ち出されるのを防止する必要上、その数値制御装置１０の再セットアップ用パスワードを変更して、現地作業員がそれまで使用していた再セットアップ用パスワードを無効にする必要がある。

【００６４】この場合、プロセッサ１１は、新しいパスワードを入力する旨のガイダンスメッセージをＣＲＴ／ＭＤＩユニット７０に表示して（ステップｃ１０）、新しいパスワードの入力を待ち（ステップｃ１１）、作業者が入力した新しいパスワードを一旦記憶してから再び新しいパスワードの入力を要求し（ステップｃ１２）、その入力を確認した後（ステップｃ１３）、１回目に入力されたパスワードと２回目に入力されたパスワードとを比較して（ステップｃ１４）、両者の一致不一致を判別する（ステップｃ１５）。

【００６５】そして、１回目に入力されたパスワードと２回目に入力されたパスワードとが一致しない場合には、パスワードを入力する作業者のキーボード等の操作にミスがあったことを意味するので、プロセッサ１１は、再び繰り返してステップｃ１０以降の処理を作業者に実行させる。

【００６６】この実施形態の場合、入力するパスワードの機密性を保持する必要上、ＣＲＴ／ＭＤＩユニット７０のディスプレイをブラインド表示にした状態でステップｃ１０～ステップｃ１４の新規パスワードの入力処理を実施するようになっており、作業者自身もキーボード等のミスタッチを自ら確認できないので、作業者にパスワードを２回入力させて数値制御装置１０側の内部処理でキーボード等の誤操作を検出するようにしているのである。

【００６７】そして、１回目に入力されたパスワードと２回目に入力されたパスワードとが一致してステップｃ１５の判別結果が真となると、プロセッサ１１は、作業者が意図する通りの再セットアップ用のパスワードが入力されたものと認め、そのパスワードをＳＲＡＭ１４に上書きすることで、それまで使用されていた再セットアップ用のパスワードを無効にし、新たに設定された再セットアップ用のパスワードを有効にする（ステップｃ１６）。

【００６８】一旦メーカー側の作業員が再セットアップ用のパスワードを書き換えてしまえば、それまで現地作業員が使用していた再セットアップ用のパスワードは無効となるので、その数値制御装置１０で生成したバックアップデータをメモリカード２０を介して他の数値制御装置に移植することは現地作業員にもできなくなる。

【００６９】

【発明の効果】本発明は、バックアップ情報に保存された固有コードと数値制御装置自体の固有コードとを比較して外部記憶媒体からのバックアップ情報の再セットアップの可否を判定するようにしているので、ＮＣメーカーが不揮発性ＲＡＭにセットアップした重要な情報がユーザーの手で不用意に他の数値制御装置に複写されて不正に利用されるのを防止することができる。しかも、正当なユーザーがデータに損傷を生じた数値制御装置の復旧作業を行う場合には、バックアップ情報に保存された固有コードと数値制御装置自体の固有コードとの一致に

より面倒なセキュリティチェックを省略して円滑な再セットアップ作業を行うことができる。

【００７０】また、バックアップ情報を保存した外部記憶媒体には、そのバックアップ情報を生成した数値制御装置の固有コードが書き込まれるので、外部記憶媒体の不正な持ち出しや貸与があった場合にも、その出所を容易に突き止めることが可能である。

【００７１】更に、再セットアップ用のパスワードを利用することにより、外部記憶媒体に書き込まれている固有コードが数値制御装置自体の固有コードと一致していない場合でも再セットアップ作業を実施できるようにしたので、数値制御装置に新機能を追加する場合のライセンス契約の更新等を始めとする現地作業員のサービス業務を能率よく実施することができる。

【００７２】更に、メーカーのみが知る第２のパスワードを使用することによって再セットアップ用のパスワードを書き換えることができるので、現地作業員の信頼性に問題が生じたような場合には、それまで使用されていた再セットアップ用のパスワードを無効にして新たな再セットアップ用パスワードを設定することができる。

【００７３】また、第２のパスワードによって再セットアップ用のパスワードの書き換えがプロテクトされるため、何らかの方法で不正な複写作業が行われた場合でも、それに使用された再セットアップ用のパスワードが外部記憶媒体またはそのデータを複写された数値制御装置にそのまま残るので、再セットアップに使用されたパスワードを確認することにより、不正な作業を行った現地作業員を容易に突き止めることができる。

【図面の簡単な説明】

【図１】本発明の不正複写防止方法を適用した一実施形態の数値制御装置の要部を示すブロック図である。

【図２】バックアップ作業時における数値制御装置の処理の概略を示す概念図である。

【図３】再セットアップ作業時の処理動作を示すフローチャートである。

【図４】数値制御装置に記憶されている再セットアップ用のパスワードを確認する場合の処理を示すフローチャートである。

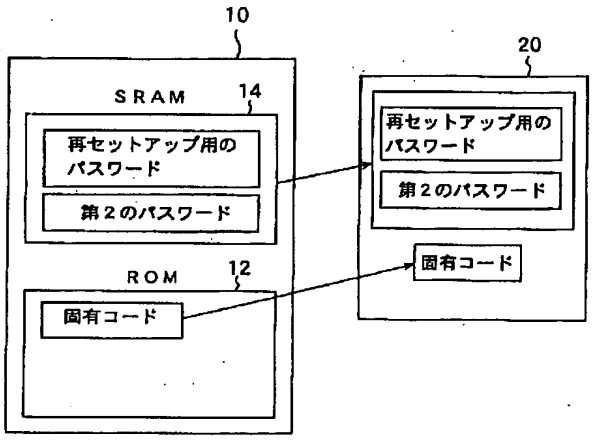
【図５】再セットアップ用のパスワードを変更する場合の処理を示すフローチャートである。

【図６】再セットアップ用のパスワードを変更する場合の処理を示すフローチャートの続きである。

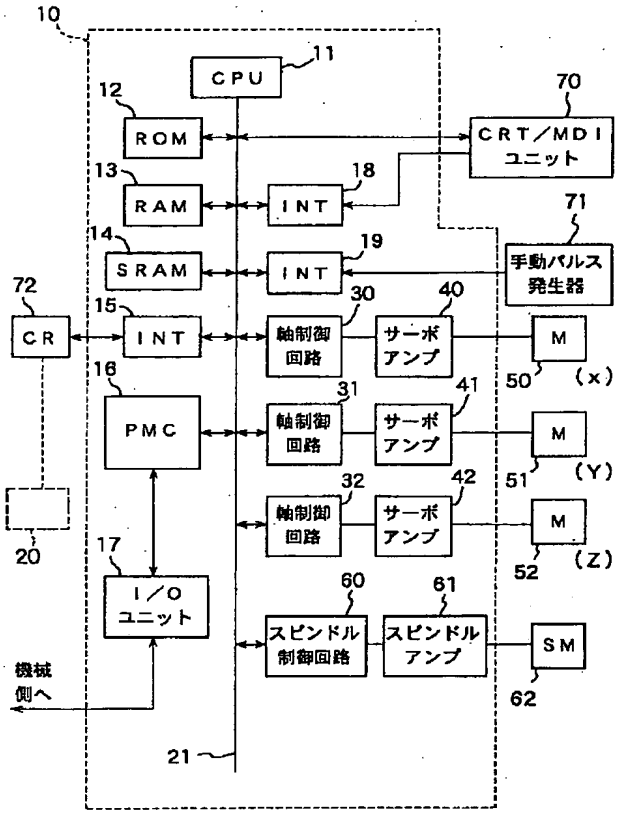
【符号の説明】

１０　数値制御装置
１１　プロセッサ
１２　ＲＯＭ
１３　ＲＡＭ
１４　ＳＲＡＭ（不揮発性ＲＡＭ）
１５　インターフェイス
１６　ＰＭＣ（プログラマブル・マシン・コントローラ）
１７　Ｉ／Ｏユニット
１８　インターフェイス
１９　インターフェイス
２０　メモリカード（外部記憶媒体）
２１　バス
３０～３２　軸制御回路
４０～４２　サーボアンプ
５０～５２　サーボモータ
６０　スピンドル制御回路
６１　スピンドルアンプ
６２　スピンドルモータ
７０　ＣＲＴ／ＭＤＩユニット
７１　手動パルス発生器
７２　外部記憶媒体のドライブユニット

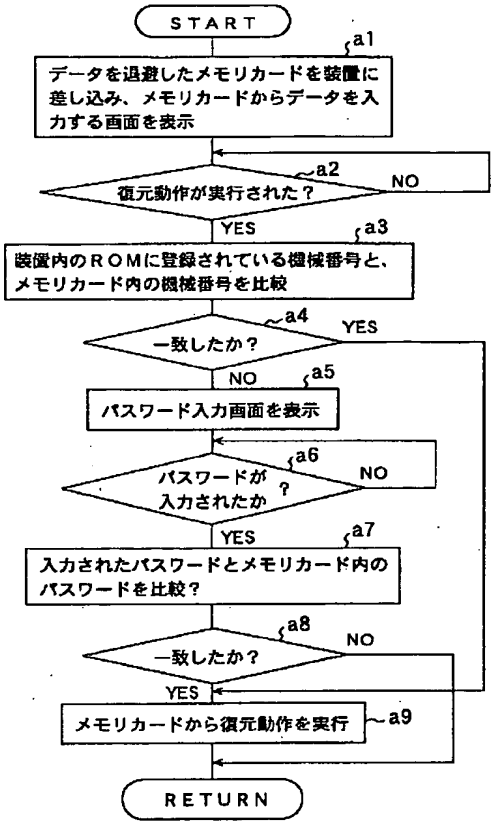
【図２】



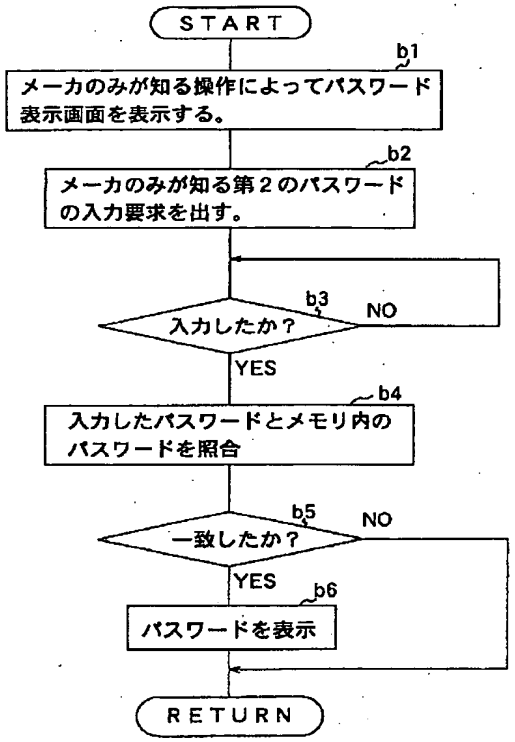
【図１】


10
CPU
11
12
ROM
70
CRT/MDI
ユニット
13
RAM
INT
18
71
14
SRAM
INT
19
手動パルス
発生器
72
CR
15
INT
30
軸制御
回路
40
サーボ
アンプ
M
50
(x)
16
PMC
31
41
51
(Y)
32
42
52
(Z)
20
17
I/O
ユニット
60
61
スピンドル
制御回路
スピンドル
アンプ
SM
62
機械
側へ
21

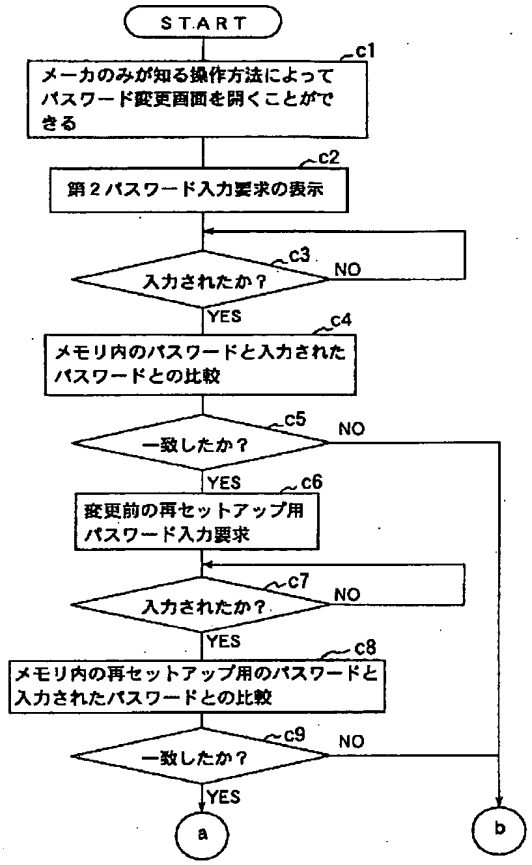
【図３】


START
a1
データを退避したメモリカードを装置に
差し込み、メモリカードからデータを入
力する画面を表示
a2
復元動作が実行された？
NO
YES
a3
装置内のＲＯＭに登録されている機械番号と、
メモリカード内の機械番号を比較
a4
一致したか？
YES
NO
a5
パスワード入力画面を表示
a6
パスワードが
入力されたか？
NO
YES
a7
入力されたパスワードとメモリカード内の
パスワードを比較？
a8
一致したか？
NO
YES
メモリカードから復元動作を実行
a9
RETURN

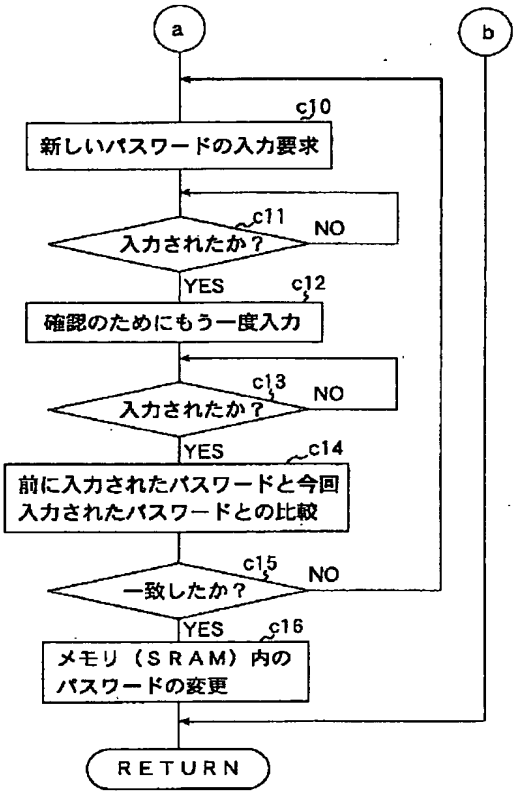
【図４】


START
b1
メーカのみが知る操作によってパスワード表示画面を表示する。
b2
メーカのみが知る第２のパスワードの入力要求を出す。
b3
入力したか？
NO
YES
b4
入力したパスワードとメモリ内のパスワードを照合
b5
一致したか？
NO
YES
b6
パスワードを表示
RETURN

【図５】


START
c1
メーカのみが知る操作方法によってパスワード変更画面を開くことができる
c2
第２パスワード入力要求の表示
c3
入力されたか？
NO
YES
c4
メモリ内のパスワードと入力されたパスワードとの比較
c5
一致したか？
NO
YES
c6
変更前の再セットアップ用パスワード入力要求
c7
入力されたか？
NO
YES
c8
メモリ内の再セットアップ用のパスワードと入力されたパスワードとの比較
c9
一致したか？
NO
YES
a
b

【図６】


a
b
c10
新しいパスワードの入力要求
c11
入力されたか？
NO
YES
c12
確認のためにもう一度入力
c13
入力されたか？
NO
YES
c14
前に入力されたパスワードと今回入力されたパスワードとの比較
c15
一致したか？
NO
YES
c16
メモリ（ＳＲＡＭ）内のパスワードの変更
RETURN